Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-001
Revision Number: 00
Issue Date: 07/25/2011

PRIVACY POLICY AND COMPLIANCE

I. Purpose

This Instruction implements Department of Homeland Security (DHS) Directive 047-01, "Privacy Policy and Compliance."

II. Scope

This Instruction applies throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII) and regarding any other activity that impacts the privacy of individuals as determined by the Chief Privacy Officer.

III. References

A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]

B. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]

C. Title 6, U.S.C., Section 142, "Privacy officer"

D. Title 44, U.S.C., Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)]

E. Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information"

F. Memorandum from the Deputy Secretary to Component Heads, "Designation of Component Privacy Officers" (June 5, 2009)

G. Information Sharing Coordinating Council, "Information Sharing and Access Agreements Guidebook and Template" (April 2010)

.

H. Privacy-related memoranda issued by the Office of Management and

Budget, including, but not limited to:

1. OMB Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007)

2. OMB Memorandum 06-20, “FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management” (July 17, 2006)

3. OMB Memorandum 06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments” (July 12, 2006)

4. OMB Memorandum 06-16, “Protection of Sensitive Agency Information” (June 23, 2006)

5. OMB Memorandum 06-15, “Safeguarding Personally Identifiable Information” (May 22, 2006)

6. OMB Memorandum 05-08, “Designation of Senior Agency Officials for Privacy” (February 11, 2005)

7. OMB Circular No. A-130, “Transmittal Memorandum #4, Management of Federal Information Resources” (November 28, 2000)

I. Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including but not limited to:

1. Privacy Policy Guidance Memorandum 2011-01, *Privacy Act Amendment Requests* (February 11, 2011)

2. Privacy and Civil Liberties Guidance Memorandum 2009-01, *The Department of Homeland Security’s Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy* (June 5, 2009)

3. Privacy Policy Guidance Memorandum 2008-02, *DHS Policy Regarding Privacy Impact Assessments* (December 30, 2008)

4. Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008)

5. Privacy Policy Guidance Memorandum 2007-02, *Regarding Use of Social Security Numbers at the Department of Homeland Security*

(June 4, 2007)

6. Privacy Policy Guidance Memorandum 2007-01, *Regarding Collection Use, Retention, and Dissemination of Information on Non-U.S. Persons* (as amended January 7, 2009)

7. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (October 31, 2008)

8. Privacy Incident Handling Guidance (PIHG) (September 10, 2007)

9. Privacy Incident Handling Guidance (PIHG) Desktop User's Guide (September 28, 2008)

10. Privacy Impact Assessment Guidance and Template (June 2010)

11. Official Guidance: System of Records Notices (April 2008)

12. Privacy Threshold Analysis Template (June 10, 2010)

IV. Definitions

A. ***Fair Information Practice Principles*** means the policy framework adopted by the Department in Directive 047-01 regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information.

B. ***Individual*** means a natural person, including a United States citizen, Legal Permanent Resident, visitor to the United States, alien, DHS employee, or DHS contractor.

C. ***Information Sharing Access Agreement (ISAA)*** means an agreement that defines the terms and conditions of information/data exchanges between two or more parties. ISAA encompasses agreements in any form, including Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, etc.

D. ***Mixed System of Records*** means a system of records (as defined in the Privacy Act of 1974, as amended, 5 U.S.C. 552a(a)(5)) that includes Personally Identifiable Information about United States Citizens, Legal Permanent Residents and visitors to the United States or aliens.

E. ***Personally Identifiable Information (PII)*** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information includes a name, social security number, date and place of birth, mother's maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (*e.g.,* a random generated number).

F. ***Privacy Act Amendment Request*** means an Individual's request that information pertaining to him or her held in a DHS system of records be amended or corrected, as provided by the Privacy Act of 1974, as amended (5 U.S.C. 552a(d)(2)).

G. ***Privacy Act Statement*** means the disclosure statement required by Section (e)(3) of the Privacy Act to appear on documents used by the Department to collect PII from individuals to be maintained in a Privacy Act System of Records.

H. ***Privacy Compliance Documentation*** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Threshold Analyses, Privacy Impact Assessments, System of Records Notices, Notices of Proposed Rulemaking for Exemption to Privacy Act System of Records (NPRM), and Final Rules.

I. ***Privacy Impact Assessment (PIA)*** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information will be used, stored, and shared, how the information may be accessed, how the information will be protected from unauthorized use or disclosure, and how long it will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

J. ***Privacy Incident*** means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to PII in usable form, whether paper or electronic, or where authorized users access PII for an unauthorized purpose. Privacy Incidents include both suspected and confirmed incidents involving PII.

K. ***Privacy Threshold Analysis (PTA)*** means both the DHS Privacy Office process to be followed and the document used to identify information technology (IT) systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what PII is collected (and from whom) and how that information is used.

L. ***Program Manager*** means the DHS employee who is responsible for the planning and operation of a DHS program.

M. ***Sensitive Personally Identifiable Information (Sensitive PII)*** means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an Individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are Sensitive PII if DHS maintains them in conjunction with other identifying information about the Individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be Sensitive PII, but could be if it is a list of employees who received poor performance ratings.

N. ***System Manager*** means the DHS employee identified in a System of Records Notice who is responsible for the operation and management of the system to which the System of Records Notice pertains.

O. ***System of Records Notice (SORN)*** means the official public notice of a DHS system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, and (4) the ways in which the information is generally shared by the Department. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS maintains about them.

V. Responsibilities

A. ***All DHS employees*** are responsible for complying with Directive 047-01 and with privacy policies and procedures issued by the Chief Privacy Officer, and for protecting PII from unauthorized use or disclosure.

B. ***Component Freedom of Information Act (FOIA) Officers*** are responsible for documenting and implementing procedures for identifying, processing, tracking, and reporting on Privacy Act Amendment Requests, where those duties are not undertaken by Component Privacy Officers.

C. ***Component Privacy Officers*** are responsible for:

1. Maintaining an ongoing review of all Component IT systems, technologies, rulemakings, programs, pilot projects, information sharing, and other activities to identify collections and uses of PII and to identify any other attendant privacy impacts;

2. Coordinating with System Managers and Program Managers, together with the Chief Privacy Officer and counsel for the Component, to complete required Privacy Compliance Documentation (1) for all proposed Component IT systems, technologies, rulemakings, programs, pilot projects, information sharing, or other activities that involve PII or otherwise impact the privacy of individuals, and (2) for any changes to operational IT systems, technologies, rulemakings, programs, or pilot projects, information sharing, or other activities that involve PII or otherwise impact the privacy of individuals;

3. Reviewing Component policies and directives to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies;

4. Overseeing Component implementation of DHS privacy policy (including all guidance documents and memoranda issued by the Chief Privacy Officer);

5. Providing the Chief Privacy Officer all Component information necessary to meet the Department's responsibilities for reporting to Congress or OMB on DHS activities that involve PII or otherwise impact privacy;

6. Overseeing the Component's implementation of Component procedures, and guidance issued by the Chief Privacy Officer, for handling suspected and confirmed Privacy Incidents; notifying the Chief Privacy Officer and other Department offices of such Incidents as Component procedures dictate; ensuring that Privacy Incidents have been properly mitigated; and recommending that the Chief Privacy Officer close Privacy Incidents upon mitigation;

7. Processing privacy complaints from organizations, DHS employees, and other individuals, whether received directly or by referral from the Chief Privacy Officer;

8. Overseeing Component privacy training and providing educational materials, consistent with mandatory and supplementary training developed by the Chief Privacy Officer;

9. Maintaining an ongoing review of all Component data collection forms, whether electronic or paper-based, to ensure compliance with the Privacy Act Statements and all implementing regulations and guidelines;

10. Reviewing Component record retention schedules for paper or electronic records that contain PII to ensure privacy interests are considered in the establishment of Component record disposition policies;

11. In consultation with the Chief Privacy Officer, advising the Component on information sharing activities that involve the disclosure or receipt of PII and participating in the review of ISAAs; and

12. Documenting and implementing procedures for identifying, processing, tracking, and reporting on Privacy Act Amendment Requests.

D. *The* ***Office of Policy*** is responsible for submitting all proposed international ISAAs to the Chief Privacy Officer for review and approval.

E. ***Privacy Points of Contact (PPOCs)*** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

F. ***Program Managers*** and ***System Managers*** are responsible for:

1. Coordinating with the Chief Privacy Officer and the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any IT system, technology, regulation, rulemaking, program, or other activity, including pilot activities;

2. Coordinating with the Chief Privacy Officer, the Component Privacy Officer or PPOC, and counsel to prepare drafts of all Privacy Compliance Documentation required when proposing, developing, or implementing or changing any IT system, technology, regulation, rulemaking, program, or other activity, including pilot activities;

3. Monitoring the design, deployment, operation, and retirement of programs and systems to ensure that the use of PII is limited to those uses described in the Privacy Compliance Documentation;

4. Establishing administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and

records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction;

5. Overseeing systems and programs that maintain PII, whether in electronic or paper form, and reporting any suspected or confirmed Privacy Incidents to the appropriate party in accordance with Component procedures for handling Privacy Incidents; and

6. In consultation with the Component Privacy Officer or PPOC and the Chief Privacy Officer, developing and implementing privacy procedures and job-related privacy training to safeguard PII in program and system operations.

VI. Content and Procedures

A. Mixed Systems of Records: DHS treats PII that it collects, uses, maintains, and/or disseminates in connection with a Mixed System of Records as a System of Records subject to the Privacy Act, regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien. Components handle non-U.S. person PII held in mixed systems in accordance with the Fair Information Practice Principles set forth in the Attachment to Directive 047-01. As a matter of DHS policy, non-U.S. persons have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act; however, this policy does not extend or create a right of judicial review for non-U.S. persons.

B. Privacy Compliance Documentation: Program Managers and System Managers complete all Privacy Compliance Documentation set forth in applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer), as follows:

1. Whenever a DHS IT system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. The Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. The Chief Privacy Officer determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation.

2. If the Chief Privacy Officer concludes that a PIA is necessary for a DHS IT system**,** technology, rulemaking, program, pilot project, or other activity that impacts the privacy of individuals, the relevant manager works with the Component Privacy Officer or PPOC, counsel for the Component, and the Chief Privacy Officer to complete the PIA in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all PIAs.

3. The Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing SORN, the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, an NPRM describing proposed Privacy Act exemptions for the System of Records and, after public comment, a Final Rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and Final Rules.

4. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.

5. Consistent with guidance issued by the Chief Privacy Officer, Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records.

C. Social Security Numbers (SSN): Department employees collect SSNs from Individuals only (1) when the collection is permitted by statute or regulation or (2) where the Chief Privacy Officer, in coordination with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines that there is other authority for the collection and that the collection is necessary. The relevant Program Manager or System Manager, in coordination with the Component Privacy Officer or PPOC, completes a PTA in accordance with guidance issued by the Chief Privacy Officer any time a new Department IT

system, technology, rulemaking, program, or other activity, or any change thereto, involves the planned collection of SSNs.

D. Information Sharing Access Agreements: Component Privacy Officers or PPOCs, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel should be involved in all phases of ISAA development. Component Privacy Officers, PPOCs, or other DHS employees, as appropriate, submit all proposed interagency ISAAs involving PII to the Chief Privacy Officer for review and approval prior to finalizing an agreement. The Office of Policy submits all proposed international ISAAs to the Chief Privacy Officer for review and approval. The Chief Privacy Officer reviews all proposed ISAAs and works with the relevant Component Privacy Officer or PPOC, or the Office of International Affairs, as appropriate, to ensure that such agreements are amended, where necessary, to fully comply with DHS privacy policy and ISAA guidance.

E. Privacy Incident Handling: The Chief Privacy Officer collaborates closely with staff of the Enterprise Operations Center and others in the Office of the Chief Information Officer, and with Component Privacy Officers, PPOCs, and staff of the Office of Inspector General, as appropriate, in handling privacy incidents. This collaboration takes place through the Privacy Incident Management Program to ensure that all DHS Privacy Incidents are identified, reported, and responded to appropriately to mitigate harm to individuals, and to DHS-maintained assets and information. The Chief Privacy Officer determines whether all required actions in connection with a Privacy Incident have been accomplished and, if so, approves closure of the Privacy Incident.

F. Privacy Complaint Handling: The Chief Privacy Officer collaborates with Component Privacy Officers to review privacy complaints received throughout DHS, and to provide redress as appropriate. Under the terms of a March 2008 Memorandum of Understanding between the Chief Privacy Officer and the DHS Inspector General, OIG has the opportunity to decide whether to conduct investigations of allegations of criminal misconduct, systemic violations, serious management problems, and allegations of non-criminal misconduct by employees at the GS-15 level or higher and all political and Schedule C employees, and, where it declines to do so, refers the matter to the Privacy Office for review and resolution.

G. Privacy Act Amendment Requests: Components identify, process, track, and report on Privacy Act Amendment Requests in accordance with applicable regulations, OMB guidelines, guidance issued by the Chief Privacy Officer, and procedures established by Component Privacy Officers or FOIA Officers. In general, the Component Privacy Officer or FOIA Officer identifies which records in a non-exempt DHS System of Records the Privacy Act Amendment Request seeks to amend, and forwards the Request to the appropriate records system manager, who confirms that the Individual submitting the Request is either the

subject of those records or the subject's designated agent or legal guardian.

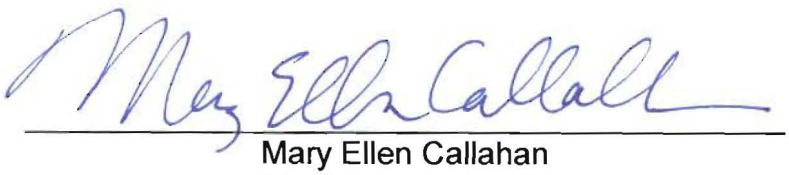
The records system manager, in consultation with the Component Privacy Officer or FOIA Officer and counsel for the Component, determines whether to amend the record(s) in question and notifies the Individual making the Request (or, as appropriate, that Individual's designated agent or legal guardian) in writing accordingly. If the decision is to amend the record(s), the approved changes are made in the relevant System(s) of Records. If the decision is to deny amendment, the Component Privacy Officer or Component FOIA Officer notifies the Individual, or his or her designated agent or legal guardian, accordingly and provides information on how to appeal the denial.

Component Privacy Officers and FOIA officers track and report the number and disposition of Privacy Act Amendment Requests to the Chief Privacy Officer as the Chief Privacy Officer may require but no less than annually.

H. Privacy Training: New DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. Employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.



Mary Ellen Callahan
Chief Privacy Officer

July 25, 2011
Date